ATLANTICO
BANCO MILLENNIUM ATLANTICO

Policy (PL)

Reference	PL-ATL-21-003	Date of Publication	07/13/2021	Version	02
owner	*Compliance Office* (COF)				

Policy on Anti - Money Laundering / Counter Terrorism and Proliferation of Weapon of Mass Destruction Financing

Contents

TITLE I - INTRODUCTION

1.1 Purpose

Banco Millennium Atlântico, SA (hereinafter referred to as ATLANTICO or Bank), adopts as a fundamental principle for its business the prevention and active detection of money laundering practices (MLP) and combat against the financing of terrorism and the Proliferation of weapons of Mass Destruction (CFT/PWMD), adopting, in this regard, internationally recognized good practices and applicable regulations in Angola. Thus, this Policy sets out the principles and rules to protect the Bank, its business, as well as prevent it from serving as a vehicle for the execution of activities related to money laundering (ML) or the financing of terrorism and Proliferation of Weapons of Mass Destruction (FT/PWMD).

In view of this, the main objectives of the Policy are to:

a) Ensure compliance with legal and regulatory requirements applicable to MLP/CTF/PWMD;

b) Contribute to the prevention and identification of situations associated with organized crime and terrorism;

c) Reduce the Bank's exposure to potential ML/FT/PWMD situations;

d) Manage the Bank's reputational risk in these matters.

The principles, rules and procedures set out herein are imperative for all ATLANTICO employees, which means that the provisions of this Policy are applicable and mandatory for all employees. This also applies to third parties who provide services to ATLANTICO, such as advisors and third parties acting on its behalf.

The structure of the policy provides for separate chapters for the main regulatory aspects related to MLP/CTF/PWDM regarding clients and operations, including their monitoring, internal communication and legal authorities, training of the employees involved, periodic review and validation by an independent entity.

1.2 Policy Implementation

Under the terms and for the purposes of this Policy, namely as regard the powers and responsibilities provided for therein, the Compliance Officer is construed as being in charge of the Compliance Office (COF).

The Bank's Bodies are responsible for implementing the Policy. The COF will be the Body responsible for the Policy, facilitating and coordinating its implementation.

1.3 Policy Approval and Review

The Executive Committee (EC) shall be responsible for the Policy, as well as any subsequent updates.

The Policy shall be reviewed annually or whenever necessary, in order to ensure that it is updating in the event of the occurrence legal and/or regulatory changes and growth of ATLANTICO's business. All future changes will be proposed by COF, in order to include updates to laws and/or regulations.

1.4 Related Policies and Procedures

This Policy is based on and is complemented by the following main ATLANTICO Policies and Procedures:

- International Sanctions Compliance Policy;
- Client Identification and Acceptance Policy ;
- MLP/CTF/PWDM and Sanctions Manual .

1.5 Measures to be taken in the event of non-compliance

Failure to comply with the requirements set out herein may expose ATLANTICO to significant regulatory and reputational damage, including fines, coercive suspension of operations or revoking of the banking license. Consequently, cases of non-compliance with the rules set out in this Policy shall be immediately communicated to the COF, which may result in disciplinary action against the parties involved and could lead to dismissal.

TITLE II - GENERAL PRINCIPLES

Regarding MLP/CTF/PWDM, ATLANTICO takes a risk-based approach, which covers its clients, Correspondent Banks and respective operations, including the aspects of identifying these entities, operations execution and monitoring of clients and operations, for what it at least considers the risk factors provided for herein.

Accordingly, increased due diligence measures should be carried out on clients and operations that, due to their nature or characteristics, may have indices of greater ML/FT/PWMD risk.

TITLE III - DEFINITIONS

This Chapter presents some definitions relevant to the understanding of the topics covered.

3.1. Money Laundering (ML)

ML can be defined as an activity through which the economic system is used, with special focus on the financial system, to conceal the true origin and/or ownership of illegal income. In this way, funds from illicit practices are concealed in a circuit of transactions and businesses with the aim of giving them an appearance of legality.

ML activity normally comprises the following three phases:

- Placement – Introduction of proceeds from criminal activity into the financial system through deposit, electronic transfers or other means. An example of placement could be the deposit of various sums in cash in a bank account;
- Circulation/Concealing – Execution of (multiple) transactions in order to separate unlawfully earned assets from their source. An example of concealment could be the conversion of cash into traveler's checks, money orders, among others;
- Integration – Reintroduction of illicit goods into the formal economy in order to create the perception of legitimacy. An example of integration could be the acquisition of goods and services.

3.2. Financing of Terrorism (FT)

FT can be defined as the provision or collection of funds, through any means, directly or indirectly, with the intention of using them, in whole or in part, for the planning, preparation or commission of a terrorist crime, regardless of the origin of such funds.

FT can occur through methods that are similar to ML. However, it is important to bear in mind that FT has characteristics that can make it even more difficult to detect, such as:

- FT can be carried out through simple transactions and for relatively small amounts, and can be easily construed as normal transactions;
- Funds used for the FT may come from legal activities;
- Although the origin of the funds may be legitimate, terrorist organizations still need to cover up the trail of these funds, in order to conceal the link between investors and the organization, or terrorist activities.

3.3. Financing for the Proliferation of Weapons of Mass Destruction (FPWMD)

FPWMD can be defined as the transfer and export of nuclear, chemical or biological weapons, related materials and their means of delivery.

3.4. Final Beneficiary (FB)

A natural person who is the ultimate owner or holder of final control of a client or persons on whose behalf a transaction is carried out, covering:

a) The natural person(s) who:

   i) Ultimately, has a shareholding in the equity of a corporate entity or control it and/or a natural person in whose name the transaction is being carried out;

   ii) Ultimately exercises effective control over a corporate entity or entity without legal personality, in situations where the

equity/control interests are exercised through a chain of equity participation or through indirect control;

iii) Ultimately owns or controls, directly or indirectly, the equity of the company or the voting rights of the corporate entity, which is not a company listed on a regulated market, subject to information requirements in line with international standards;

iv) Is entitled to exercise or who exercise significant influence or who controls the company regardless of the level of participation.

b) In the case of legal entities that manage or distribute funds, they are natural person or persons who:

i) Benefit from their assets when the future beneficiaries have already been determined;

ii) Are considered as the category of persons for whose main interest the corporate entity was incorporated or carries on its activity, when the future beneficiaries have not yet been determined;

iii) Exercise control over the assets of the corporate entity.

3.5. Politically Exposed Persons (PEPs)

According to the Act nr. 05/2020 of 27 January , nationals or foreigners who hold or have held prominent public positions in Angola, or in any other country or jurisdiction or in any international organization.

Thus, regardless of their nationality, for the purposes of classifying PEPs, the following fall under:

a) For the purposes of this Act, the following are considered high political or public positions:

i) President of the Republic or Head of State;

ii) Vice-President of the Republic;

iii) Prime Minister or Head of Government;

iv) Ancillary Organs of the President of the Republic, or members of the Government, namely Ministers of State, Ministers, Secretaries of State and Deputy-Ministers and other similar positions or functions;

v) Members of Parliament, members of Parliamentary Chambers and similar institutions;

vi) Judges of High Courts and the Court of Appeal, whose decisions cannot be appealed, save for exceptional circumstances;

vii) Judges in the Public Prosecutor's Office at the same level as judges of courts of justice as set out in the foregoing paragraph;

viii) Ombudsman and Deputy Ombudsman;

ix) Members of the Council of the Republic, the National Security Council and other State Advisors;

x) Members of the National Electoral Commission;

xi) Members of the Supreme Judicial Councils and the Public Prosecutor's Office;

xii) Members of management and supervisory bodies of central banks and other regulatory and supervisory authorities in the financial sector;

xiii) Heads of diplomatic missions and consular posts;

xiv) Generals of the Armed Forces and Commissioners of the Security Forces and Internal Order;

xv) Members of the Board and audit bodies of public companies and of companies with entirely or mostly public equity, public institutes, public associations and foundations, public establishments, regardless of their designation, including the management bodies of companies that are part of the local business sectors;

xvi) Members of the Board of Directors, Directors, Deputy Directors and/or persons occupying equivalent positions in an international organization;

xvii) Members of executive bodies of the Board of political parties;

xviii) Members of local administrations and local government;

xix) Religious Leaders.

b) Within the scope of this Act, family members and people that are very close to the aforementioned individuals are also treated as politically exposed persons, namely:

i) The spouse or cohabiting partner;

ii) Relatives, up to the 3rd degree of the collateral line, and similar people up to the same degree, their respective spouses or cohabiting partners;

iii) People with recognized and close personal relationships;

iv) People with recognized and close corporate or business relations, namely:

a) Any natural person who is notably known as the joint owner of a corporate entity with the holder of a high political or public position or who has close business relations with him;

b) Any natural person who owns the equity or voting rights of a corporate entity or the assets of a center of collective interests without legal personality, who is notably known, with the sole beneficial owner being the holder of a high-ranking political or public office.

The Bank constitutes as PEPs accounts in which there is at least one stakeholder (e.g. Director, Manager, or FB) identified in the account opening documents that fall into this category. In such cases, in line with what applies to other high-risk ML/TF clients, the following procedures shall be carried out:

- Application of enhanced due diligence procedures;
- Approval of the opening of an account by the EC, after the opinion of the COF;

- Application of enhanced monitoring measures on client transactions.

3.6. High Risk Countries

Some countries may be qualified as high risk countries for ML/TF/PWMD, due to political upheavals, armed conflicts, high level of organized crime, recognized involvement in the production or trafficking of narcotics, some offshore jurisdictions considering their respective characteristics (e.g non-cooperating jurisdictions).

In this regard, keeping close business relations with nationals and/or residents of a country with high risk ML/TF, or those who regularly do business with this type of country, may expose ATLANTICO to greater risk of ML/TF.

Thus, ATLANTICO maintains an updated list of countries, classifying them according to ML/TF risk, taking into account the recommendations of the Government of Angola and other institutions (including FATF, UN, OFAC, OFSI and EU). This list is used for the purposes of calculating the clients' ML/TF risk and is also considered when monitoring the respective transactions.

3.7. Unacceptable Clients

ATLANTICO does not accept account opening of unidentified clients or numbered accounts. Furthermore, the following cases are considered as clients of unacceptable ML/FT/PWMD risk:

a) Clients related to countries, entities or individuals sanctioned by the UN, the Government of Angola, among other entities;
b) "Pseudo" Banks;
c) Anonymous entities, or those controlled by anonymous individuals;
d) Lack of information on the nature and purpose of the business and origin and destination of the client's funds.

TITLE IV – ORGANIZATION AND CONTROL PROCESSES

4.1 Organization

The organic and functional model of compliance with MLP/FT/PWMD implemented by the ATLANTICO ensures that:

a) Directors and other managers are aware of their responsibilities and receive the information necessary to identify, manage and control ML/FT/PWMD risks;
b) ML/FT/PWMD risks are periodically monitored and assessed by the EC and COF;
c) There are controls in place to assess whether the COF and the other Organs are performing their functions effectively.

In ATLANTICO, compliance risk management, in terms of MLP/CTF/PWDM, consists of, without limiting its core, the following:

d) EC functions and responsibilities;
e) COF functions and responsibilities;
f) The functions and responsibilities of each of the functional areas, particularly their heads;
g) The monitoring carried out by the Audit Department (AD);
h) The functions and responsibilities of the Bank's employees in general.

4.1.1 Executive Committee

The ATLANTICO EC is ultimately responsible for ensuring compliance with MLP/CTF/PWDM legal and regulatory obligations, and ensuring the implementation of policies, procedures, systems and controls to mitigate ML/FT/PWMD risks.

The EC shall:

a) Define, formalize, implement and periodically review policies and processes related to compliance risk management, transactions with related parties, prevention of conflicts of interest and prevention and detection of suspicious operations of criminal activities or fraud situations;
b) Carry out effectiveness tests on MLP/CFT Controls;
c) Analyze and discuss the reports produced by the key functions of the internal control system, i.e. internal audit, compliance and risk management.

4.1.2 *Compliance Office*

The person in charge of COF is the Compliance Officer of ATLANTICO. The *Compliance Officer* must be given the room for independence, authority and access to the other Bodies of the Bank, as well as the necessary resources to perform his duties.

The COF is the organic unit responsible for implementing the MLP/CTF/PWDM Compliance Program, as well as monitoring its internal compliance,

ensuring that the procedures and systems put in place for this purpose are effective and meet the legal obligations to which ATLANTICO is subject. The COF shall analyze potentially suspicious situations, as well as report them, both internally and to the responsible entities. Furthermore, the COF shall be responsible for establishing the *Key* Performance Indicators (KPIs) and Key Risk Indicators *(KRIs*) to be reported. The main objective of the KPIs shall be to measure the performance of the Compliance Program against the MLP/CTF/PWDM and the KRIs measure compliance against the main associated risks. The following reports shall be produced:

1. **Annual reports** – shall present a more operational aspect of MLP/CFT activities, including KPIs/KRIs, such as: i) number of alerts generated and respective review results, respectively within the scope of client and transaction monitoring ii) number of reports sent to the FIU. These half-yearly reports will be addressed to the Executive Committee (EC), all COF employees and the Audit Department (AD);
2. **Annual reports** – should present a more strategic aspect of MLP/FT activities, including the KPIs/KRI exemplified above, in addition to others with a more comprehensive view, as well as enhancements identified and/or implemented. These annual reports will essentially be addressed to the EC, the AD and the COF.
3. **Annual reports to regulators** – should be sent to regulators, namely the National Bank of Angola and the Capital Markets Commission with information required by them on AML.

Thus, the COF shall:

4. Monitor the procedures put in place by the heads of the functional areas as related to MLP/CTF/PWDM;
5. Coordinate the before and after control of clients and operations in accordance with the approved risk assessment;

6. Streamline the process of reporting suspicious transactions to the Financial Information Unit (FIU);
7. Define, propose and coordinate the process of reporting information to the Management bodies of ATLANTICO on suspicious operations and on the activity carried out by them.

4.1.3 Persons Responsible for Functional Areas

The heads of each of ATLANTICO's functional areas shall:

a) Implement, control and verify the degree of compliance with prevention and control procedures in its functional unit, and shall keep the COF informed of the occurrences that may be found;
b) Know and monitor the occurrences related to ML/FT/PWMD within its functional unit, and shall keep the COF informed;
c) Suggest and implement, in collaboration with the COF, additional control procedures and precautionary measures that it may deem necessary, based on the specifics of its functional unit, with the aim of detecting and preventing suspicious operations.

4.1.4 Audit Department

The AD is responsible for regularly monitoring and testing the design, effectiveness and effectiveness of ATLANTICO's MLP/CTF/PWDM program, thus providing additional assurance to the EC in these matters.

The head of AD shall:

a) Monitor the performance of the functional areas and the COF;
b) Carry out design and effectiveness tests to MLP/CTF/PWDM controls.

To this end, ATLANTICO shall:

a) Continuously evaluate the applicability of the procedures in place;
b) Define and monitor the main risks and respective indicators associated with ML/FT/PWMD;
c) Ensure an effective training strategy;
d) Periodically conduct effectiveness tests on the procedures and systems adopted.

Furthermore, and in order to obtain a deeper and more independent view of the effectiveness and efficiency of the MLP/CTF/PWDM Program, ATLANTICO shall also regularly conduct specialized external audits on these matters.

4.1.5 Employees

ATLANTICO employees play an important role with regard to MLP/CTF/PWDM. As such, all ATLANTICO employees are responsible for ensuring that they comply with the provisions of this Policy.

In carrying out their daily duties, employees shall:

a) Remain vigilant to the possibility of occurrence of ML/FT/PWMD situations;
b) Immediately report all suspected ML/FT/PWMD to the COF;
c) Comply with all procedures relating to client identification, opening and maintenance of accounts, monitoring of accounts, maintenance and recording of documentation and collaboration in providing information to the COF;
d) Ensure that clients are not alerted on any reports to the authorities about their transactions.

Employees are also responsible for completing all MLP/CTF/PWDM training assigned to them, and subsequently diligently applying the knowledge acquired in those training sessions, in accordance with their respective roles/responsibilities.

4.2 Control Processes

ATLANTICO has internal control mechanisms and procedures for the assessment and management of ML/FT/PWMD risk, supplemented with a communication system (internal and for the legal authorities), in order to mitigate or prevent this risk.

For control purposes, ATLANTICO shall continuously ensure the applicability of the procedures in place, defining and monitoring the main ML/FT/PWMD indicators and risks.

4.2.1 ML/TF Risk Assessment

ATLANTICO is responsible for adopting mechanisms and procedures for internal control, risk assessment and management, internal audit and communication that enable the fulfillment of the legal duties to which it is subject, and that are capable of preventing the occurrence of operations related to the ML/FT/PWMD.

In the context of the departmental organization referred to in the previous point, ATLANTICO adopts internal control mechanisms and procedures for the assessment and management of Compliance risk in the MLP/CTF/PWDM, complemented with a communication system (internal and for the legal authorities), to mitigate or prevent this risk. The design of the processes takes into account the primary activities aimed at executing the operations, identifying and accepting its stakeholders, as well as the control activities carried out by the execution areas, the COF and the AD.

To this end, ATLANTICO defines its controls based on an annual assessment of the respective exposure to ML/FT/PWMD risks. The risk assessment methodology is based on the following risk factors identified by ATLANTICO:

a) Type, size and complexity of the activity carried out by the subject entity;

b) Countries or geographic areas in which the subject entity operates, directly or through third parties, whether or not belonging to the same group;

c) Business areas carried forth by the subject entity, as well as products, services and operations provided;

d) Type of client;

e) Client history;

f) Type, size and complexity of the activity carried out by the client;

g) Countries or geographic areas in which the client operates directly or through third parties, whether or not belonging to the same group;

h) Form of establishment of the business relationship;

i) Geographic location of the client of the obliged entity or where it is domiciled or in some way operates;

j) Transactions carried out by the Client;

k) Distribution channels of the products and services provided, as well as the means of communication used to contact clients;

l) Shareholder profile;

m) The suitability of computer tools and applications;

n) The level of knowledge and integrity Board members and employees.

ATLANTICO's risk is mitigated by the MLP/CTF/PWDM internal control system.

The COF is responsible for conducting risk assessment. In the event that the assessment identifies that certain risks are not being adequately mitigated, the COF shall propose an action plan to implement new controls and/or review existing ones.

ATLANTICO shall ensure that it has all the relevant information about the people and entities with which it relates. Thus, ATLANTICO shall ensure that it adopts a risk-based due diligence methodology. With this approach, counterparts that pose high ML/FT/PWMD risks should be considered as high risk, and enhanced due diligence and monitoring should be carried out. ATLANTICO shall regularly update the due diligence information of counterparts during business relations in order to ensure an accurate risk classification. The due diligence shall be reviewed if any event indicates *that* the risk associated with the client has changed (e.g. blocked or even rejected transactions, or negative information from public sources of information). In the event of clients classified as being of high risk, the due diligence shall be reviewed at least annually.

4.2.2 Screening

Screening plays an important role in identifying risks associated with ML/FT/PWMD. Thus, ATLANTICO shall implement controls that allow the screening of clients and their relevant related parties (e.g FBs, signatories, attorneys, among others), transactions, suppliers and employees, in line with the provisions of this Policy and the Compliance Policy in view of International Sanctions.

The automatic screening systems used by ATLANTICO shall meet the minimum requirements for fuzzy matching. This mechanism allows the configuration of a percentage of correspondence, and only alerts with a similarity level higher than the defined value will be investigated, thus allowing the assignment of a probability sorting for each case resulting from the screening. Screening systems shall be calibrated according to ATLANTICO's risk assessment.

Screening shall be conducted on:

a) All new clients and their relevant related parties, suppliers and employees;
b) All Bank clients, at least monthly;
c) When there are changes in counterpart information;
d) When new additions are made to the Sanctions and PEPs lists;
e) In transfers and payments issued/received from clients that have their destination/origin in other banks.

For the purposes of this Policy, it should be noted that in addition to the possible self-declaration of a client as a PEP, it is the screening that acts as a control for the identification of PEPs for the subsequent enhanced due diligence (EDD) process. and EC approval. In the same context, this is the system used to identify sanctioned parties, with which ATLANTICO cannot establish business relations or, where these relations are prior to the sanction, they shll be frozen and reported to the authorities.

4.2.3 Compliance Risk Assessment Methods

The assessment of compliance risk in MLP/CTF/PWDM, within the framework of Angolan regulations for the acceptance and monitoring of clients, execution and monitoring of operations and reporting to the competent supervisory and supervisory authorities, is based on an ordinal scale of increasing risk, according to the characteristics of clients and operations, the level of which determines the final decision (i.e. accept/not accept, execute/not execute, report/not report) and/or the actions of the various stakeholders in the process (e.g. employees of the Business Departments, respective leaderships, COF, AD and CE), which can take the form of alerts and/or enhanced diligences.

The form, risk factors and respective estimates, decision levels and reporting duties associated with the compliance risk are to be done in form of

an autonomous and substantiated proposal, prepared by the COF and addressed to the ATLANTICO EC for approval.

4.2.4 Client Risk Rating

The reputational defense processes of ATLANTICO and MLP/CTF/PWDM, framed within a logic of differentiation and grading of ML/FT/PWMD risk, only become truly effective with the application of classification, analysis and monitoring policies that permanently allow for the risk level of the entity to be understood. Under these circumstances, all ATLANTICO clients are classified as being:

1. Low risk: if the entities, sources of wealth or origin of funds are easily identifiable or whose operations are usually adequate and in apparent compliance with the known profile of the client, whether an individual or a corporate entity and that in the risk classification established by ATLANTICO are classified as having a low risk level;

2. Medium risk: when there are factors capable of leading to the aggravation of a risk considered non-negligible for ATLANTICO, such as the client's profession or activity, the entity's core business, the inexistence of some identification data and the transactional profile in the use of products and services, classified by ATLANTICO as having a medium-low or medium-high risk level;

3. High risk: for all those entities that fit the criteria that ATLANTICO has defined to consider the acceptance of clients as conditioned, whenever there are factors considered to strongly increase risk, such as geographical criteria, high-risk activities risk (e.g. non-religious and charitable organizations, foundations, *money* service businesses, etc.), PEPs, clients whose risk is political (due to concrete occurrences that indicate high risk) or even those that by their nature may reveal, directly or indirectly, a greater risk for engagement in unlawful acts, classified by ATLANTICO with a high risk level.

For this purpose, ATLANTICO has a ML/FT/PWMD Risk Matrix, which allows the automatic determination of the client's risk level both at the time of opening an account and during the business relationship. Below are some of the factors that are considered in this matrix:

a) Type of Client activity;
b) Client's nationality and country of residence/operation;
c) The type of products that the client intends to use;
d) PEP status;
e) Private *client*;
f) Type of company, for corporate entities;
g) The length of the business relationship.

The COF may review and change the risk factors listed above according to its risk assessment of ATLANTICO's business, developments in National/International regulations, compliance with good international practices, technological developments and others for reasons that allow the mitigation of risk to the reputation of ATLANTICO.

4.3 Client Monitoring and Control

ATLANTICO has computer tools that allow it to automatically control and monitor clients and their transactions within the framework of MLP/CTF/PWDM.

Monitoring and control activities include, but are not limited to, the following practices:

a) Monitoring and control of clients and transactions with a high ML risk level;
b) Monitoring and control of transactions involving high risk ML countries;
c) Monitoring and control of complex and/or extraordinary transactions;
d) Monitoring the consistency between transactions and the information collected on the client's activity, risk profile and financial assets on a permanent basis. This activity involves not only occasional transactions (daily alerts) but also the temporary analysis of the client's transactional profile in terms of average amounts and number of executed transactions (monthly alerts);
e) Control of transactions that exceed a predetermined amount (by client's risk level) and whether they are consistent with the client's profile;
f) Monitoring and control of related occasional transactions, which, as a whole, exceed the legal limit required for identification of the client;
g) Monitoring and control of transactions involving entities subject to various sanctions and embargoes, included in the lists of entities issued by the UN, EU, OFAC, among others (with the aim of controlling compliance with these

restrictions enacted internationally), as well as internal lists, preventing/restricting their transactions or forcing enhanced steps. In this context, ATLANTICO sets priorities for action in real time, according to the reason that gave rise to the "screening" of the operation;

h) Control of the completion and updating of the client's information and documents that shall be kept in paper or digital format, as well as the additional information that shall be included in electronic transfer of funds;
i) Control of transactions presented by unreliable means or not in-person;
j) Control of trade finance transactions. Validation of operation taking into account the identification of the parties involved, the goods in question and countries of origin and destination, as well as whether the operation fits into the activity of the parties involved. It should also be noted that, within the scope of Compliance in the face of international sanctions and embargoes, all those involved in the letter are screened against international listings.

Regardless of the criteria mentioned above and whatever the level of ML/FT/PWMD risk of the client, the country involved in the transaction or the complexity and its danger, special attention shall be paid to all conducts and/or activities whose characterizing elements may increase the risk or probability of a relationship with ML/FT/PWMD crimes, and information and documentary evidence, compliance and economic rationale of the transactions submitted for analysis shall be collected.

If there is a transaction that indicates ML/TF practices, the Bank must, if possible, refrain from executing it and, in all cases, the COF shall always report the situation to the FIU.

TITLE V – CLIENT IDENTIFICATION AND ACCEPTANCE 5.1

Know Your Client (KYC)

The due diligence procedures conducted aimed at knowing the client are a crucial requirement of the MLP/CTF/PWDM Policy, in order to prevent the use of the financial system for ML/FT/PWMD. These procedures shall be carried out at the beginning of the business relationship, updated regularly and evaluated in conjunction with the client's transactional profile.

This process includes:

a) The account opening process;

b) The assessment of the level of risk of ML/FT/PWMD;
c) Regular updating of client information, taking into account the respective ML/FT/PWMD risk level;
d) Continuous monitoring of client activity, also taking into account the respective level of ML/FT/PWMD risk.

As mentioned above, ATLANTICO applies a ML/FT/PWMD risk rating system applicable to all clients, FBs and other counterparts, which, acting in real time for the purpose of assigning a risk level, is based on the weighting of the client's characteristics known during the KYC procedure (e.g. job, country of residence, PEP status, among others). This system automatically allows each client to be assigned an adjusted and differentiated risk level. As the ML/FT/PWMD risk rating process for clients is dynamic, the appropriate procedures shall be applied to all existing clients and accounts according to the risk assigned to them or those whose risk is increased according to the criteria decided upon by ATLANTICO, in line with the law and existing regulations.

5.2 The Account Opening Process

The client Identification and Acceptance Policy stipulates the guiding principles on the type of clients with which ATLANTICO is willing to initiate or maintain business relations, namely for the purposes of MLP/CTF/PWDM. The aforementioned Policy spells out the account opening process that includes, among other procedures:

a) The identification and verification (ID&V) of the client's identity, using documentation and reliable sources;
b) Collection of information on the type and purpose of the business relationship (e.g. the client's activity and sources of income, and intended products and services);
c) Obtaining of information on the control structure and carrying out ID&V procedures on FBs of clients classified as Entities;
d) Identification of clients that are considered PEPs.

Under certain circumstances, the account opening process shall include:

e) EDD procedures for clients classified as high ML/TF risk;
f) Simplified due diligence for cases provided for by Law;
g) The hierarchical approval of clients (e.g. PEPs and other clients classified as high ML/FT/PWMD risk).

The information collected shall be updated regularly and/or based on certain events, and shall be used to calibrate the monitoring of client transactions.

Thus, in accordance with existing laws and regulations, ATLANTICO employees shall conduct the ID&V of clients, their respective FBs and other stakeholders, whenever:

1. A business relationship is established and/or at the time of opening an account, in person or remotely;
2. Occasional transactions are carried out in which the amount, individually or jointly, is equal to or greater, in local or foreign currency, to the equivalent of USD 15,000;
3. There are suspicions that the operations, regardless of their amounts, are related to a ML/FT/PWMD crime;
4. The operation, regardless of its nature and amount, is related to a country or territory considered non-cooperating.

If the Client (or his representative) refuses to provide the respective identification or the identification of the person for whom he is actually representing, ATLANTICO, in accordance with the provisions of paragraph 1 of article 15 of Act Nr. 05/2020 of 27 January , has the obligation to:

- Refuse to open the account;
- Refuse the initiation of the business relationship;
- Refuse to carry out any operations;
- Terminate the business relationship with that client.

While the guidelines on MLP/CTF/PWDM are applicable to all new clients, they shall also apply to existing clients based on weighted materiality and risk criteria.

5.3 Simplified Diligence

When a demonstrably low risk of money laundering, financing of terrorism and proliferation of weapons of mass destruction is identified in business relationships, in occasional transactions or in operations carried out, ATLANTICO takes into account, namely, the origin or destination of the funds, as well as the factors referred to in paragraph 2 of article 12 of the Law No. 05/20 of January 27 .

Subjected entities shall consider, among others, the following factors:

a) The purpose of the business relationship;
b) The level of assets per client or volume of operations carried out;
c) The regularity or duration of the business relationship.

In analyzing the risks of money laundering, financing of terrorism and the proliferation of weapons of mass destruction, which may lead to the taking of simplified measures, the subjected entities and the inspection and supervisory authorities take into account other situations indicative of potentially lower risk that may be identified by the respective inspection and supervisory authorities.

5.4 Enhanced Diligence

EDD consists of developing in-depth procedures in order to obtain a more complete understanding of clients whose ML/FT/PWMD risk level is considered high.

These additional measures may consist of:

a) Request for additional information and documentation about the client, in order to understand the nature of its activity, source of income, funds, assets to be used in the business relationship, transactional profile, among others;
b)
c) Conducting research on independent sources of information in order to verify if there is adverse information on the client (e.g. if it is involved in criminal investigations or associated with accused parties in such investigations);
d)
e) Enhanced monitoring of the business relationship, namely through continuous in-depth monitoring of the operations associated with the client.

These procedures must be carried out on all ML/FT/PWMD high risk clients including but not limited to:

f) PEPs;
g) Clients who carry out operations done remotely;
h) Non-profit organizations, charities or religious entities;
i) Establishment of banking correspondence relationships and any others designated by the inspection or supervisory authorities of the respective sector, provided that they are legally authorized to do so;

j) Private segment clients.

In this regard and given their characteristics, certain clients and operations pose an increased ML/FT/PWMD risk, for which reason closer and continuous monitoring should be carried out from the opening of account and throughout the course of the business relationship.

It is therefore the duty of ATLANTICO to verify the relationship of consistency between the knowledge that the Bank has of its clients, their respective businesses and risk profiles with the activities carried out by them, by monitoring their banking operations and, where necessary, determining the source of the funds.

5.5 Visits to Clients

Client visits are the best opportunity to verify and update the information obtained when opening an account or initiating a relationship. Collecting information about the client and carrying out visits is part of the continuous process of information gathering that should commence at the beginning of the relationship with the client and must be maintained throughout the duration of the relationship. business.

The client contact functional units can visit clients at their place of work in order to verify the type and volume of their activities, as well as the source of income and update all the necessary information. The visits and discussions with clients shall be recorded in the Client Relationship Management system.

5.6 Duty of Identification in Occasional Transactions

Whenever ATLANTICO intends to, either in-person or using remotely, make occasional transactions of an amount equal to or greater, in local currency, than the equivalent of USD15,000.00 (Fifteen Thousand American Dollars), regardless of whether the transaction is carried out through a single operation or through several operations that appear to be related to each other or occasional transactions of any amount on which they suspect a possible connection with ML/FT/PWMD crimes, ATLANTICO must obtain in the least the identification documents of such clients and their representatives, at the beginning and during the operation, pursuant to the terms set out in the Client Identification and Acceptance Policy (without precluding the duty of refusal and communication provided for in Act Nr. 05/20 January 27).

5.7 Duty of Refusal

In accordance with Act nr. 05/20 of 27 January, the duty of refusal shall be carried out whenever the requirements set out in articles 11 to 14, on the obligation of identification and diligence, cannot be fulfilled, therefore the following shall be done:

a) Refuse to open the account;
b) Refuse to initiate the business relationship;
c) Refuse to carry out the transaction;
d) Terminate the business relationship.

The employee shall stop execution of such an operation and immediately communicate the instruction/operation to the COF, which shall decide whether the instruction/operation should or should not be refused.

TITLE VI – CONDUCT OF TRANSACTIONS

6.1 Principle of Universality

All transactions conducted by ATLANTICO are analyzed and their MLP/CTF/PWDM risk is assessed under the terms set out herein. For this purpose, ATLANTICO continuously analyzes transactions carried out.

6.2 Acceptance of Transactions

ATLANTICO and all its employees play an active role in identifying a suspicious transaction. These operations can be defined as:

1. Transactions that deviate from the normal patterns of account activity. For example:
   a) Unexpected movement on inactive accounts;
   b) Significant total amount, transacted through deposits/withdrawals in cash of small amounts, made in several branches and sent to the same account.
2. Any complex transaction or unusually high amount for the client's profile. For example:
   a) Attempt by an individual, without financial capacity, to carry out a significant transaction, concealing the true sender/beneficiary of the transaction;
   b) Use of open accounts for receipts and payments of large amounts without such being suited to the business done by the respective account holders.

3. Transactions without apparent economic, commercial or lawful cause. For example:
   a) Cash deposits/withdrawals of large amounts, made by individuals or companies, whose activity should not involve cash transactions but using other means of payment/receipt;
   b) Significant increases in the bank balance through cash deposits that are systematically transferred to the account of another ATLANTICO client or to another Bank.

Transactions done or brokered by ATLANTICO are subject to assessment during their implementation, thus making them dependent on the outcome of such assessment, pursuant to the rules and principles established herein.

4. ATLANTICO shall truncate transactions of which it has knowledge or well-founded suspicions of such being connected to the practice of ML/FT/PWMD crime, namely when:
   a) The identification instruments of the client, its legal representative or the FB of the transaction or assets are not provided, as well as when there are doubts as to the veracity of the client identification data;
   b) Sufficient information is not provided to identify the FB of the funds;
   c) No information is provided regarding the client's ownership and control structure, type and purpose of the business relationship and source/destination of the funds;
   d) Within the framework of MLP/CTF/PWDM compliance risk management, transactions carried out by ATLANTICO are subject to:
      1. General control conducted by any ATLANTICO employee in contact with the transaction and respective leadership;
      2. Prior control carried out by the COF before the respective execution;
      3. Post control carried out by the COF after the execution of the operation;
      4. Any communication to the FIU by the COF.

6.3 Special Duty of Due Diligence

Transactions that, due to their nature, complexity, purpose, unusual nature of the client's mode of operating, amounts involved, frequency, economic and financial status of the clients involved or the means of payment used, are likely to be connected to ML/FT/PWMD.

Without precluding risk assessment, pursuant to the provisions set out herein, additional due diligence measures shall always be applied to the following transactions:

a) Conducted remotely, especially those that are anonymous;
b) Conducted with PEPs;
c) Within the scope of cross-border correspondence banking relationships with institutions established in third countries, for which information must be obtained on the nature of their activity, internal control processes in terms of MLP/CTF/PWDM and characteristics of the supervision to which they are subject.

6.4 Correspondent Banks

The COF is responsible for coordinating all actions and communications associated with MLP/CTF/PWDM carried out within the scope of correspondence relations.

A Correspondent Bank is a financial institution with which ATLANTICO establishes a partnership agreement, in order to represent or be represented.

1. Correspondent bank relationships carry a high ML/FT/PWMD risk for ATLANTICO and, as such, additional procedures and controls should be carried out to mitigate them, namely:
   a) Application of EDD procedures which, among others, should include obtaining information on the nature of the Correspondent Bank's activity, the respective shareholders and regulatory compliance, as well as on the adequacy and effectiveness of its internal control system for MLP/CFT /PWMD and Sanctions;
   b) Approval of the correspondence banking relationship by the Board, after the COF's opinion;
   c) Assessment, based on publicly known information, of the correspondent bank's reputation and the characteristics of its supervision;
   d) Application of enhanced monitoring measures on transactions.

Additionally, all correspondence banking relationships are subject to specific, detailed written contracts.

ATLANTICO takes the necessary measures in accordance with existing rules and good practices on the establishment or maintenance of relationships with Correspondent Banks, particularly complying with the provisions of articles 2, 14, 33 and 34 of Act Nr. 05/20, of 27 January , and with the rules established by notice nr. 2012/25 of the BNA.

TITLE VII - MONITORING OF CLIENTS, CORRESPONDENT BANKS AND TRANSACTIONS

7.1 Principle of Universality

All clients, Correspondent Banks and their transactions are subject to MLP/CTF/PWDM compliance risk monitoring mechanisms, pursuant to the provisions set out herein.

7.2 Form and Timing of the Monitoring Process

At ATLANTICO, the monitoring process is conducted continually, and is particularly important when there are significant changes to the risk profile of clients, Correspondent Banks or when the logic of their transactions changes.

7.3 Duty of Due Diligence

1. During the conduct of the duty of monitoring, ATLANTICO shall, on a regular basis and depending on the risk level of each client and/or Correspondent Bank:
   a) Take appropriate measures to understand the client's ownership and control structure, in the case of a corporate entity, as well as in the case of Correspondent Banks;
   b) Obtain information on the purpose and intended nature of the business relationship;
   c) Obtain information on the source and destination of funds transacted within the scope of a business relationship or in the execution of an occasional transaction, when the risk profile of the entity involved or the characteristics of the operation thus justify;
   d) Continuously monitor the business relationship in order to ensure that such transactions are compatible with the entity's knowledge of the activities and risk profile of the client and/or Correspondent Bank;
   e) Keep the information obtained during the course of the business relationship up to date.

7.4 Risk Factors

1. Risk assessment in the monitoring of clients considers the following as risk factors, in the least, namely:
   a) Registration on lists produced by leading international institutions;
   b) Legal or reputational information (e.g. legal proceedings, ongoing investigations) on the client, Correspondent Bank or supplier;

c) Any change that has impact on the remaining risk factors contained in the initial risk assessment.

2. Risk assessment monitoring of operations considers the following, in the minimum, as behavioral risk factors, namely:
   a) The amount and frequency of transactions;
   b) The amount and frequency of transactions to countries and territories considered to be at high risk of ML/FT/PWMD;
   c) Significant fluctuations in the amounts and/or type of transactions ordered.

TITLE VIII - COMMUNICATION

8.1 Duty of Information and Collaboration

All ATLANTICO employees are obliged to report any situation that may constitute a ML/FT/PWMD crime. The communication shall be sent to the COF in accordance with the procedure established in the MLP/CTF/PWDM and Sanctions Manual, providing as much information as is available. Consequently, and after analysis, ATLANTICO informs the FIU whenever there is reason to suspect that a transaction that has been carried out, is in progress or has merely been attempted, is likely to constitute a ML/FT/PWMD crime, in accordance with and respecting the principles spelt out in the existing laws. To this end, the COF shall submit a Suspicious Transaction Report (STR) to the FIU.

ATLANTICO provides all the assistance required by the competent judicial authorities or by the competent authorities (BNA, Capital Markets Commission and the FIU) for the supervision and inspection of compliance with legally established duties.

In possession of the information identified and detected, the Compliance Officer initiates the procedure for reporting suspicious clients and transactions to the FIU under the terms of the legally established protocol of communication with this Unit. The performance of the Compliance Officer is independent, as provided for under existing laws.

Furthermore, ATLANTICO communicates to the FIU all cash transactions equal to or greater than, in local currency, the equivalent of 15.000.00 (Fifteen Thousand American Dollars), and is obliged to report all transactions identified in article 17 of Act nr. 05/20 of 27 January and the consequent attached table.

8.2 Communication Process

ATLANTICO has procedures in place that enable it to respond timeously to requests for information submitted by judicial authorities and other competent authorities under the terms set out in this chapter.

8.3 Detection by Employees

All ATLANTICO employees are responsible for ensuring that they comply with the provisions of this Policy.
Employees in client contact and relationship areas who detect a suspicious ML/FT/PWMD transaction or behavior must report them to the person responsible for their functional unit, who will then forward the information to the COF, which is responsible to analyze it, conduct risk assessment and take possible actions.

In carrying out their daily duties, employees shall:

a) Be on the watch out for the possibility of occurrence of ML/FT/PWMD situations;
b) Immediately report all suspected ML/FT/PWMD internally;
c) Comply with all procedures on client identification, account opening and maintenance, account monitoring, documentation maintenance and recording, and collaboration in the provision of information to the area responsible for internal reporting;
d) Ensure that clients are not alerted on any reports sent to the authorities or internal investigations of their transactions.

Employees are also responsible for completing all MLP/CTF/PWDM training assigned to them, and subsequently diligently applying the knowledge acquired in such training, in accordance with their respective roles/responsibilities.

8.4 Duty of Secrecy

Members of the respective governing bodies, or who occupy Board, management or leadership positions, their employees, representatives and other persons who provide services to them on a permanently, temporarily or occasionally to ATLANTICO, cannot disclose to the client or to the third parties, that they have transmitted legally required communications or that a criminal investigation is in progress.

8.5 Duty of Abstention

ATLANTICO shall truncate transactions that may reveal suspicions of ML/FT/PWMD in the context of Angolan laws. Whereby it is not possible to truncate the transaction or, after consulting the FIU, it is considered that the stopping it may hinder the investigation of the transaction, it may be concluded and ATLANTICO shall immediately provide all information concerning such transaction to the FIU.

TITLE IX - REVIEW OF POLICIES AND PROCESSES BY AN INDEPENDENT AND QUALIFIED ENTITY

The Policy shall be reviewed every year or whenever necessary, in order to ensure it is up to date on possible legal and/or regulatory changes and developments in ATLANTICO's business.

Periodic review by an independent entity is also provided for. The scope of the independent entity's work includes:

a) Review and assessment of the validity of policies, namely in the event of occurrence of changes to Angolan regulations or in guidelines issued by leading international institutions;
b) Tests of the processes and procedures established to assess their compatibility and consistency with formally approved policies.

The AD shall prepare the proposal for the contracting of an independent entity, after consulting the Supervisory Authority and the COF. It shall be submitted for the approval of the Audit and Internal Control Committee, and the EC shall subsequently be informed. When choosing the entity, its reputation, knowledge and experience in similar processes will be considered.

TITLE X - TRAINING

A training in MLP/CTF/PWDM matters falls within the following:

a) Regular training courses on MLP/CTF/PWDM will be provided to all ATLANTICO employees, including EC members;
b) Training courses shall, at the barest minimum, focus on matters related to the client identification and acceptance, transaction execution, client and transaction monitoring and identifying and reporting of suspicious transactions;
c) To the extent necessary, the COF may develop training tools and clarify doubts on the subject of MLP/CTF/PWDM and the measures put in placed by ATLANTICO to manage the associated risk.

ATLANTICO employees whose duties include opening accounts or new products, or who may be in contact with activities or transactions that are more prone to ML/FT/PWMD, shall receive adequate training for the performance of their duties.

Employees who work in specialized business areas (e.g. COF and AD) and whose functions are responsible for MLP/CTF/PWDM shall undergo specialized training on a regular basis.

Records of training contents and attendance of training courses shall be kept for a period of 5 (five) years.

TITLE XI - DOCUMENT CONSERVATION

ATLANTICO stores documents for a minimum period of 10 (ten) years from the moment the transaction is carried out or after the end of the business relation, and ensures their easy access. The documents to be kept are the following:

a) Hard copy of documents or other technological devices testifying to the identification and of all business correspondence exchanged with clients;
b) Originals or copies with identical legal validity as documents that show evidence of the operations/transactions, which are sufficient to revisit each operation;
c) Copy of all business correspondence exchanged with clients;
d) Originals or copies with identical legal validity as the documents that show evidence of information obtained under special duties of due diligence;
e) Copy of reports sent to the FIU and the competent authorities;
f) Records of results of internal analyses, as well as a record of the reasons given by the subjected entities for the decision not to inform the FIU or other competent authorities on the outcome.

ATLANTICO shall establish documented procedures, systems and controls in order to ensure proper storage and access to the above listed documents. All documents shall be legible, auditable and retrievable.

TITLE XII - SANCTIONS REGIME

Pursuant to applicable laws, ATLANTICO and its employees may be held liable for violations of the provisions of these Policies.

Although the financial entity is responsible for offences committed by its employees, individual persons may also be held liable.

In this regard, Act Nr. 05/2020, of January 27 and the Act Nr. 1/2012, of 12 January , provide for offenses punishable by fines and/or ancillary penalties, to be applied depending on the gravity and persons involved in such situations, such as:

- Fines in the amount equivalent in local currency to:
  - USD25,000 to USD2,500,000, if the agent is a corporate entity;
  - USD12,500 to USD1,250,000 if the agent is a natural person.
- Warning or prohibition from exercising the profession or activity to which the offence relates;
- Punishment with a fine or prison term of up to three years for anyone who, even with mere negligence, reveals or acts in favor of the discovery of the identity of the person who provided information to the FIU;
- Prison term of two to eight years for anyone who colludes with the author or participant in an ML/FT/PWMD offence.

TITLE XIII - GLOSSARY OF TERMS

ATLANTIC or Bank	Banco Millennium Atlântico, SA
ML *(ML)*	Money Laundering *(Branqueamento de Capitais)*
FB *(BEF)*	Final Beneficiary *(Beneficiário Efectivo Final)*
BNA	National Bank of Angola *(Banco Nacional de Angola)*
CDD	*Client Due Diligence*
EC *(CE)*	Executive Committee (*Comissão Executiva)*
CTF	Combating of Terrorism Financing (*Combate ao Financiamento do Terrorismo)*
COF	*Compliance Office*
AD *(DAU)*	Audit Department (*Direcção de Auditoria)*
STR	Suspicious Transaction Reporting
EDD	*Enhanced Due Diligence*
ESAAMLG	*Eastern and Southern Africa Anti-Money Laundering Group*
FT	Financing of Terrorism

FATF (GAVI)	Financial Action Task Force *(Grupo de Acção Financeira Internacion)*
ID&V	Identification and Verification

KPI	*Key Performance Indicators*
KRI	*Key Risk Indicator*
KYC	*Know Your Client / Counterpart*
KYT	*Know Your Transaction*
OFAC	*Office of Foreign Assets Control*
OFSI	*Office of Financial Sanctions Implementation*
UN	United Nations Organization
MLP (PB)	Money Laundering Prevention
PWMD *(PDAM)*	Proliferation of Weapons of Mass Destruction
PEP	Politically Exposed Person
HRP (PPRE)	High Risk Personnel
EU	European Union
IFU (FIU)	Financial Information Unit
USD	American Dollar

TITLE XIV - ANNEXES

14.1 Main Legislation

International:

- Provisions and recommendations issued by national and international entities such as the FATF – Financial Action Task Force and ESAAMLG – Eastern and Southern Africa Anti-Money Laundering Group, namely the 40+9 FATF/FATF Recommendations on MLP/CFT;
- United Nations Convention Against Illicit Traffic in Narcotics Drugs and Psychotropic Substances;
- United Nations Convention against Transnational Organized Crime.

National:

- ☐ Act Nr. 05/20, of January 27 – Law on combating money laundering and the financing of terrorism and the proliferation of weapons of mass destruction;
- ☐ Act Nr. 1/12, of January 12 – Law on the designation and execution of international legal acts;

- ☐ Act Nr. 12/2015, of 17 June – Baseline Law on Financial Institutions;
- ☐ Presidential Decree Nr. 212/13 of December 13 – Organizational Statute of the Financial Information Unit and the Supervisory Committee;
- ☐ Presidential Decree Nr. 214/13 of December 13 – Regulations on the Designation and Execution of International Legal Acts;
- ☐ Act nr. 2 /2013 of April 19 – Regulates the obligation of financial institutions to establish an internal control system supervised by the BNA;
- ☐ Notice Nr. 10/2016 of July 18 – Establishes the general terms and conditions for opening, operating and closing bank deposit accounts;
- ☐ Instruction Nr. 24/2016 of 16 November – Enhanced due diligence duties;
- ☐ Instruction Nr. 02/2018 of January 19 – Foreign Exchange Policy;
- ☐ Instruction Nr. 13/2018 of September 19 – Foreign Exchange Policy;
- ☐ Directive No. 03/DSI/2012 of 24 July – Identification and communication of designated persons, groups and entities;
- ☐ Directive Nr. 04/DSI/2012 of 24 July – Freezing of funds and economic resources;
- ☐ Directive Nr. 02/DSI/2013 of 1 July – Guidelines for the implementation of a program to prevent money laundering and terrorist financing;
- ☐ Directive Nr. 02/DRO/DSI/15 of 10 December – Guidelines on MLP/CFT in with respect to Correspondent Banks and Client Banks;
- ☐ Notice Nr. 14/2020 of May 29 - Rules for the Prevention and Combat of Money Laundering and Terrorism Financing;
- ☐ Instruction Nr. 20/2020 of December 9 – Report on the Prevention of Money Laundering, Financing of Terrorism and Proliferation/Risk Assessment and IT Tools and Applications;
- ☐ Instruction Nr. 04/2021 of February 24 - Partial Amendment of Instruction nr. 20/20 of 9 December on the Report on the Prevention of Money Laundering, Financing of Terrorism and Proliferation.

14.2 General Risk Indicators

- Clients who maintain business relations carry out occasional transactions or carry out general transactions that – due to their nature, frequency, amounts involved or any other factor – are inconsistent with their profile;
- Clients who, without plausible explanation, handle in cash:
  - In unusual amounts;
  - In amounts not justified their profile;

  - Packed or packaged in an unusual way;
  - In poor condition;
  - Represented by small denomination banknotes, with the aim of exchanging them for higher denomination banknotes.
- Clients who, in some way, try to persuade ATLANTICO employees not to observe any legal obligation or internal procedure of ML/FT/PWMD prevention;
- Clients who are reluctant or refuse to provide identification details/evidence means/other information documentation or to carry out the verification procedures considered needed by ATLANTICO for:
  - Their identification, that of their representative and/or FB;
  - Understanding their ownership and control structure;
  - Knowledge of the nature and purpose of the business relationship;
  - Knowledge of the source and destination of funds;
  - The characterization of their business.
- Clients who are reluctant or refuse to provide original documents or documents of equivalent value;
- Clients who are reluctant or refuse to update their information;
- Clients who are reluctant or refuse to establish face-to-face contacts with ATLANTICO;
- Clients who provide identification details, means of proof or other information details with the following features:
  - Poor authenticity credibility;
  - Poorly explicit content;
  - Difficulty for of verification by ATLANTICO;
  - Unusual features.
- Clients who present different identification documents each time they are requested by ATLANTICO;
- Clients who, in the exercise of their activity, use pseudonyms, nicknames or any other alternative expressions to their real name or designation;
- Clients who postpone or fail to deliver documentation to be submitted to ATLANTICO after the establishment of the business relationship;
- Clients who seek to suspend or change the business relationship or the occasional transaction after being asked for identifying details,

respective means of proof or other information relevant to their knowledge;

- Clients who do not want to receive any correspondence at the declared address;
- Clients who, without any apparent relationship between them, have the same addresses or contact details (telephone number, fax number, e-mail address or others);
- Clients whose address or contact details (telephone number, fax number, e-mail address or others) prove to be incorrect or are permanently out of service, especially when the attempt for ATLANTICO to contact them occurs shortly after the establishment of a business relationship;
- Clients whose address or contact details (phone number, fax number, email address or others) change frequently;
- Clients who appear to be acting on behalf of a third party, without, however, disclosing it to ATLANTICO or, even where such circumstance is disclosed, refuse to provide the necessary information details about the third party on behalf of which they are acting;
- Clients who seek to establish close relationships with ATLANTICO employees;
- Clients who seek to restrict any contacts they establish with ATLANTICO to a specific employee or employees, especially when – in the absence of such employees – they decide not to execute and/or suspend transactions;
- Clients who show unusual knowledge of ML/FT/PWMD related legislation;
- Clients who show an unusual interest and curiosity in knowing ATLANTICO's policies, procedures and internal control mechanisms for the prevention of ML/FT/PWMD;
- Clients who, within a short period of time, started similar business relationships with different Banking Financial Institutions;
- Clients who carry out their activity in successive different locations, in an apparent attempt to avoid detection by third parties;
- Clients who repeatedly transact in lower amounts than the limits that would require the conduct of identification procedures;
- Clients who acquire assets of significant value and who, in the short term and for no apparent reason, sell them off;
- Clients who, on the same day or within a short period of time, carry out transactions at different ATLANTICO Branches/Centers;

- Clients who present unclear or inconsistent explanations about transactions or who claim to have little knowledge of their purpose;
- Clients who give excessive and unsolicited explanations about transactions;
- Clients who show nervousness and/or an unusual urgency in the execution of transactions;
- Clients connected to suspicious ML/FT/PWMD transactions reported by ATLANTICO to the competent authorities;
- ☐ Clients connected to suspicious ML/FT/PWMD transactions, reported by the supervisory authorities under articles 13 and 16 of Act Nr. 05/20 - of 27 January - and that are known to ATLANTICO;
- Clients who are or have been under watch for the practice of criminal activities, in particular ML/FT/PWMD or any of the criminal offenses underlying these two types of crime (and which information is directly known to ATLANTICO or acquired through a credible public source);
- Clients expressly mentioned by the competent authorities as possibly being connected to ML/FT/PWMD transactions;
- Clients who carry out any type of financial activity without being duly authorized or qualified for such;
- Transactions that reveal a level of complexity that is apparently unnecessary for the achievement of the purpose for which they are intended, particularly due to the number of financial transactions, financial institutions, accounts, people involved and/or countries or jurisdictions;
- Transactions the economic purpose or rationality of which are not evident;
- Transactions the frequency, uniqueness or strangeness of which do not have a plausible explanation considering the client's profile;
- Transactions that appear to be inconsistent with the current practice of the client's sector of business or activity;
- Transactions involving "shadow companies";
- Transactions that have no connection with the client's known activity, which involve persons or entities related to publicly recognized countries or jurisdictions such as:
    - Narcotics production/trafficking sites;
    - People that have high corruption rates;
    - Money laundering platforms;
    - Promoters or supporters of terrorism;
    - Promoters or supporters of the proliferation of weapons of mass destruction.
- Transactions that do not have any connection with the client's known activity, which involve persons or entities related to countries, territories

or regions with special tax regimes, or other countries or jurisdictions with highly restrictive legislation on bank secrecy;
- Business relations or occasional transactions that seek to camouflage the identity of FBs, namely through complex corporate structures.

14.3 Risk Indicators Related to Manual Foreign Exchange Transactions

- Operations broken down into several purchases/sales in an attempt to avoid compliance with legal and regulatory obligations stipulated for operations that reach a certain amount;
- Transactions that are inconsistent with the Client's known activity, due, in particular, to their amount or frequency;
- Transactions executed based on an exchange rate that is more favorable to the Financial Institution than the advertised rate and/or the payment of commissions at an amount greater than the amount due, as proposed by the client;
- Transactions in which clients wish to exchange large sums in a given foreign currency for another foreign currency;
- Transactions with non-resident clients who appear to travel to the country with the clear purpose of making purchases/sales of currency;
- Frequent transactions with banknotes with a reduced face value or with currencies with limited international circulation;
- Transactions in which clients give instructions to the Financial Institution, in terms of the currency equivalent being subsequently delivered to a third party;
- Operations in which clients insist on receiving the equivalent amount by check from the Financial Institution, this practice is not usually adopted by the same;
- Transactions in which clients request the receipt of the equivalent value, in foreign currency, in notes with the highest possible face value;
- Operations in which clients request the receipt of the equivalent value in several postal orders of small amounts, to be sent to several beneficiaries.

14.4 Risk Indicators Related to Employees of Financial Institutions

- Employees who repeatedly fail to observe legal obligations or internal procedures regarding the prevention of ML/FT/PWMD;
- Employees who establish relationships of familiarity and closeness with clients that go beyond the normal standard of the duties assigned to them, or are who are inconsistent with the internal practices of the ATLANTICO;

- Employees who show a pattern of social behavior or other external signs that are not compatible with their financial status and which are known to ATLANTICO.

14.5 Other Risk Indicators

- Transactions related to the sale of real estate in which:
  - The sale value is much higher than market values;
  - Payment is made by a cashier's check or by an endorsed check in favor of a third party with no apparent connection to the transaction;
  - The payment is made in cash, particularly where such funds are remitted from a current account held by a third party without apparent relationship with the buyer,
  - The transacted property was recently acquired by the seller.
- Transactions related to non-profit organizations when:
  - The nature, frequency or amount of transactions are not consistent with the size of the organization, with its objectives and/or with its known activity;
  - The frequency and amount of operations suddenly increase;
  - The organization maintains large funds in its current account for long periods of time;
  - The organization only raises contributions from people or entities that are not resident in Angola;
  - The organization apparently has few or no means human and logistical personnel assigned to the respective activity;
  - The organization's representatives are not resident in Angola, especially when large amounts are transferred to the country of residence of such representatives;
  - The organization has some form of connection with countries or jurisdictions that are publicly recognized as places of narcotics production/trafficking, such as having high levels of corruption, money laundering platforms, promoters or supporters of terrorism or promoters or supporters of proliferation of weapons of mass destruction.
- Clients who suddenly substantially increase the number of visits to their rental safes;
- Clients who carry out high-value transactions using prepaid cards or who purchase a large number of prepaid cards from the same Financial Institution.

IMPLEMENTATION

This Policy enters into force as of the date of its publication, pursuant to employees being informed on its content to this end.

Prepared by: *Compliance Office*

Banco Millennium Atlântico